

REMARKS

Claims 28-52 are currently pending in the subject application, and are presently under consideration. Claims 1-25 are rejected. Claims 1-8 and 11-27 have been cancelled. New claims 28-52 have been added, which correspond to originally filed claims 1-8 and 11-27, respectively, to correct numbering errors in the originally filed claims. In particular, the new claims have been added to correct the omission of claims 9 and 10. Favorable reconsideration of the application is requested in view of the amendments and comments herein.

I. Rejection of Claims 1, 8, 14 and 20 Under 35 U.S.C. §103(a)

Claims 1, 8, 14 and 20 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,658,568 to Ginter, et al. ("Ginter") in view of U.S. Patent No. 6,233,341 to Riggins ("Riggins"). Withdrawal of this rejection and allowance of claims 28, 35, 41, and 47 are respectfully requested for at least the following reasons.

New claims 28, 35, 41, and 47 (cancelled rejected claims 1, 8, 14, and 20) recite a method of automatically obtaining a second certificate for a user using a first certificate comprising the authentication of both a user's server identity via a server certificate of a user server and a user's identity via the user's first certificate, and creating a secure data channel between the registration server and the user server. Ginter teaches the issuance by one certifying authority using a trusted database to obtain another certificate from another certifying authority (col. 84, ll. 64-67). In the method taught by Ginter, one certifying authority validates a user's identity and creates an identity certificate which is used to validate the user's identity to a different certifying authority, with a trusted database, which subsequently issues another certificate to the user without the need for physical evidence of identity (col. 84, line 67 - col. 85, ll. 1-15). Hence, Ginter teaches that only the user's identity is required for validation to acquire the certificate from the certifying authority, and is completely silent on the use of a server certificate to authenticate a user's server identity. Ginter, thus does not teach or suggest that both the user's identity and the user's server identity are authenticated using a user's first certificate and a server certificate of the user server, as recited in claims 28, 35, 41, and 47. Ginter is also

completely silent as to the creation of a secure channel between a registration server and a user server. Ginter, therefore, does not teach or suggest the recitations of claims 28, 35, 41, and 47.

The addition of Riggins does not cure the aforementioned deficiencies of Ginter to teach the recitations of claims 28, 35, 41, and 47. Riggins discloses the installation and enablement of a temporary certificate in a remote site. The Office Action relies upon Riggins to teach the creation and transmission of a public/private key pair. However, neither Ginter nor Riggins, alone or in combination with each other, teach or suggest authentication of both a user's server identity via a server certificate of a user server and a user's identity via the user's first certificate, and creating a secure data channel between the registration server and the user server, as recited in claims 28, 35, 41, and 47. Accordingly, claims 28, 35, 41, and 47 are not obvious over Ginter in view of Riggins. Withdrawal of the rejection of claims 28, 35, 41, and 47, as well as claims 29-34, 36-40, 42-46, and 48-52, which depend from claims 28, 35, 41, and 47, respectively, is respectfully requested.

II. Rejection of Claim 2 Under 35 U.S.C. §103(a)

Claim 2 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Ginter in view of Riggins as applied to claim 1 above, in further view of U.S. Patent No. 6,625,734 to Marvit, et al. ("Marvit"). Withdrawal of this rejection and allowance of claim 29 is respectfully requested for at least the following reasons.

New claim 29 (cancelled rejected claim 2) recites sending a backup copy of the private key from the authority to a key recovery authority. New claim 29 depends from new claim 28, and should thus be patentable for the reasons described above with regard to claim 28. Additionally, Marvit teaches that a key may be saved to a backup key repository to ensure that the key can be made available should the key be inadvertently deleted from key repository 106 (col. 18, ll. 30-33). However, Marvit teaches that "a digital signature of a message is generated at step 4, at the time that user 102 encrypts the message based on the message ID and key that are received from key repository 106." (col. 17, ll. 63-66). It is known in the art that public keys are used to encrypt messages while private keys are used to decrypt messages. Thus, because

Marvit teaches that the key stored in key repository 106 is used to encrypt messages, the key taught by Marvit is not a private key. Therefore, Marvit does not teach or suggest sending a backup copy of the private key from the authority to a key recovery authority, as recited in claim 29. Accordingly, claim 29 should be allowed over the cited art. Withdrawal of this rejection is respectfully requested.

III. Rejection of Claims 3-25 Under 35 U.S.C. §103(a)

Claims 3-25 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Ginter in view of Riggins as applied to claims 1, 8, 14 and 20 above, in further view of U.S. Patent No. 5,373,561 to Haber, et al. ("Haber"). Withdrawal of this rejection and allowance of claims 30-52 are respectfully requested for at least the following reasons.

New claims 30-34 depend from claim 28, new claims 36-40 depend from claim 35, new claims 42-46 depend from claim 41, and new claims 48-52 depend from claim 47. Haber teaches a system for certifying or validating the existence or occurrence of a recorded document or event by relying upon cryptographic assumptions to establish the basis for such a certification or validation. However, Haber does not cure the aforementioned deficiencies of Ginter in view of Riggins. In particular, Haber does not teach or suggest the authentication of both a user's server identity via a server certificate of a user server and a user's identity via the user's first certificate, and creating a secure data channel between the registration server and the user server, as recited in claims 28, 35, 41, and 47, from which claims 30-34, 36-40, 42-46, and 48-52 depend. Therefore, claims 30-34, 36-40, 42-46, and 48-52 should also be allowed over the cited art. Withdrawal of this rejection is respectfully requested.

Serial No. 09/704,417

Docket No. NG(MS)7188

CONCLUSION

In view of the foregoing remarks, Applicant respectfully submits that the present application is in condition for allowance. Applicant respectfully requests reconsideration of this application and that the application be passed to issue.

Please charge any deficiency or credit any overpayment in the fees for this amendment to our Deposit Account No. 20-0090.

Respectfully submitted,

Date 7/19/09

Christopher P. Harris
Christopher P. Harris
Registration No. 43,660

CUSTOMER No.: 26,294

TAROLLI, SUNDHEIM, COVELL, & TUMMINO L.L.P.
526 SUPERIOR AVENUE, SUITE 1111
CLEVELAND, OHIO 44114-1400
Phone: (216) 621-2234
Fax: (216) 621-4072